ISSN:2229-6093

Deepak Chayal et al, Int. J. Comp. Tech. Appl., Vol 2 (4), 803-806

Security Enhancement in MANET with 4G

Mr. Deepak Chayal*, Dr. Vijay Singh Rathore**
Research Scholar, Professor***
*Department of Computer Science, NIMS University, Jaipur**
*Department of Computer Science, S.K. College, Jaipur***

ABSTRACT

Ad hoc networks seem to have commercial potential in business meeting places, hotspots, home environments and personal areas allowing fast exchange of documents during meetings, exchange of data when playing games in a group of users and connecting home appliance among other uses. In the context of the heterogeneous and integrated 4G environment, ad hoc networking is considered an important solution to extend the radio coverage of wireless systems and multimedia Internet services to wireless environments. 4G Technology is basically the extension in the 3G technology with more bandwidth and service offers in the 3G. The expectation for the 4G technology is basically the high quality audio/video streaming over end to end Internet Protocol. As the need for fastest communication is the foremost priority of present era also the need of quick data transfer, distant business correspondence by sharing data becomes very important. In this paper, we've dealt with the primary challenge of building security in MANETs and also maintain the information required to properly route traffic. Along with this, we have also discussed about the potentials of 4G technology.

1. Introduction to Available Wireless Technologies

Traditionally, the service provision in 2G networks, e.g. GSM, has been mainly based on voice services, closed business model support and limited operator differentiation due to a narrow set of offered services. Actually, mobile service provision is facing important advancements towards more flexible business models, with the introduction of new 2.5G/3G generations of mobile communication systems, like GPRS, UMTS and CDMA2000. Unfortunately, these 2.5/3G networks entail limitations to fulfill requirements imposed by current mobile users specially with the "anytime, anywhere with anybody" type of communication. Since 1970s, the research of ad hoc networking was mainly large scale networks for emergency/rescue and military purposes respectively for disaster and battlefield communication applications. *Large scale isolated ad hoc networks* are not suited to transport a large amount of data due to their very low traffic performance, slow topology convergence and security problems. However, these could be used to transport very urgent short messages (e.g. to inform about the location of an accident or to transmit tactical commands). Since 1990s, *small isolated ad hoc networking* has been experiencing a growing interest in the commercial and residential areas due the proliferation of small information computational devices and the emerging wireless technologies (IEEE 802.11, Bluetooth). This development is driven by the need to exchange digital information among people in direct contact enabled by ad hoc networking among a number or wireless nodes. Small In the context of the heterogeneous and integrated 4G environment, ad hoc networking is considered an important solution to extend the radio coverage of wireless systems and multimedia Internet services to wireless environments [1],[2]. In these *integrated ad hoc networks* mobile ad hoc hosts and routers can gain Third/fourth generation cellular networks (3G/4G) are broadband wireless mobile networks that has evolved from the 1st to the 2nd and 3rd generation networks. The still evolving 4th generation network is expected to be deployed in later 2011.

2. The Fourth Generation Technology

4G is short for Fourth (4th) Generation Technology. 4G Technology is basically the extension in the 3G technology with more bandwidth and service offers in the 3G. The expectation for the 4G technology is basically the high quality audio/video streaming over end to end Internet Protocol. If the Internet Protocol (IP) multimedia sub-system movement achieves what

it going to do, nothing of this possibly will matter. 4G is intended to provide:

- High speed
- High capacity
- Low cost per bit
- IP based services for video, data and voice (VoIP).

4G is all about integrated, global network that is based on an open system approach. At the moment we have several technologies each capable of performing some of functions like broadband data access in mobile or nomadic environment, supporting voice traffic using voice over IP etc[3]. But what we really need is a deployment of new technologies that allow merging, bridging and integrating all these repeated system into an information delivery system of the twenty first century. 4G stands for Fourth Generation and is the latest technology with high speed transferability of data with security measurements. It is coming with wireless broadband for the instant download. Talking about the standard of 4G technology, so far, two technologies are supposed to be the features of 4G.

2.1.WiMAX

WiMAX stands for Worldwide Interoperability of Microwave Access previously worked as fixed wireless facility under the 802.16e band. Now the modified standard 802.16m has been developed with the properties of speed, wide spectrum, and increase bandwidth. 4G has an advantage of having the WiMAX as a product because IEEE has introduced and released it already, therefore its economic as there is no need to pay for its manufacturing price. 4G supports two basic equipments;W iMAX Network system (network infrastructure) and mobile phone set. Smartphones with Wireless Access introduced in the market are the model 4G mobiles. These smartphones are equipped with the wireless internet accessibility and there is no fear of losing connection while travel from one tower to another tower range. WiMAX or mobile structural design will become progressively more translucent, and therefore the acceptance of several architectures by a particular network operator ever more common.

2.2. LTE

Parallel to WiMAX, LTE (Long Term Evolution) is introduced by Verizon. LTE is considered to be promising high data transfer speed. LTE is supposed to provide internet facility using both systems. It has the ability of transition from one mode to another. LTE is developed on radio waves technology. This not only increases the speed but also the amount of data allowed through the same bandwidth and results into lower cost. As LTE is compatible with 3G technology so, it not only increases the speed but also prevents the need of new network and can work through the same infrastructure. LTE will not only support the functions of 3G but also incorporate some newer ones. LTE is using MIMO (Multiple input multiple output) and is able to send and receive huge data. It is negative in the sense that it will overload the base stations networks.

4G Technology offers high data rates that will generate new trends for the market and prospects for established as well as for new telecommunication businesses. 4G networks, when tied together with mobile phones with in-built higher resolution digital cameras and also High Definition capabilities will facilitate video blogs. After successful implementation, 4G technology is likely to enable ubiquitous computing, that will simultaneously connect to numerous high data speed networks offering faultless handoffs all over the geographical regions. Many network operators possibly utilize technologies for example; wireless mesh networks and cognitive radio network to guarantee secure connection & competently allocates equally network traffic and bandwidth.

3. Security Enhancement in MANET with 4G

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Authentication research has determined that for a positive identification, elements from at least two, and preferably all three, factors be verified. The three factors (classes) and some of elements of each factor are:

3.1.The Ownership Factors:

Something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone).

3.2. The Knowledge Factors:

Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question))

3.3. The Inherence Factors:

Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

At small scale, the identity verification can be managed by the nodes themselves, as handshaking by virtue of their proximity [4], but at relatively larger scale it becomes complex and the nodes identity verification demands the authentication involvement of TTP [5]. There are schemes that are based on the concept of self-organization in MANETS [6] thoroughly without TTP connection where the identity is resolved by the nodes themselves or some hybrid form of above two schemes might be used [4]. The 4G system was originally envisioned by the Defense Advanced Research Projects Agency. The DARPA selected the distributed architecture, end-to-end Internet protocol (IP), and believed at an early stage in peer-to-peer networking in which every mobile device would be both a transceiver and a router for other devices in the network eliminating the spoke-and-hub weakness of 2G and 3G cellular systems. Since the 2.5G GPRS system, cellular systems have provided dual infrastructures: packet switched nodes for data services, and circuit switched nodes for voice calls. In 3g and 4G systems, the circuitswitched infrastructure is abandoned, and only a packetswitched network is provided. This means that traditional voice calls are replaced by IP telephony. Cellular systems such as 4G allow seamless mobility; thus a file transfer is not interrupted in case a terminal moves from one cell (one base station coverage area to another, but handover is carried out. The terminal also keeps the same IP address while moving, meaning that a mobile server is reachable as long as it is within the coverage area of any server. In 4G systems this mobility is provided by the mobile IP protocol, part of IP version 6, and while in earlier cellular generations it was only provided by physical layer and data link layer protocols. In addition to seamless mobility, 4G provides flexible interoperability of the various kinds of existing wireless networks, such as satellite, cellular wireless, WLAN, PAN and systems for accessing fixed wireless networks. 4G stands for the fourth-generation cellular network. Although it is generally agreed that 4G is going to offer better communication technology than 3G, it is still undefined as to which areas should be really improved upon, and in which ways, from 3G. Researchers are often pointing towards integration whereas business institutions are working on upcoming technologies that will make 4G more attractive to the business community by implementing it more customer-friendly. New support for mobility is the primary concern of Hussian *et. al.* [7] and they pointed out insufficient 3G mobility constrained by bandwidth that should be significantly increased. According to them, the significant progress that 4G can achieve in the area of mobility is unifying different and currently separated environments into a single fixed OWA (Open Wireless Architecture) that will achieve high connectivity by accessing all kinds of networks. Providing single terminal that will effectively access the best available internet connection will increase and speed up device usability under 4G. Integration is the key concept in defining 4G capabilities since we should support all kinds of multimedia by offering single access to all wireless networks. Understanding the significance of unifying Wi- Fi, WiMax and Cellular networks into one product, Woerner and Howlader proposed that the most important factor of 4G will be "seamless integration of wireless networks" based on flexibility of the software radio technology, with improved bandwidth capacity, and improved routing techniques allowing multi-hop peer-topeer networks. Due to the lack of single military scenario where and how 4G will be used, it is critical that future wireless technology will be capable of effortlessly accessing all kind of radio communications. Bauer *et. al.* addressed that enhanced cellular range and capacity, supported by Wi-Fi and WiMAX networks is the vision of 4G. However, considering the fast development of WiMAX networks, and the increasing range of Wi-Fi standards, they argue that these new wireless networks can in the future substitute cellular networks such as the current 3G. They also addressed that it is "misleading" calling the evolution of cellular technology in terms of generations because this would "suggest a linear progression" which is not the case. Finally, they also evaluated business opportunities of 4G pointing out on establishing a global standard, along with open architecture, and supporting multiple interfaces all over the world, as the keys to economical success. Steer [7] addressed 4G is officially designated by IEEE as "Beyond 3G." Characterized by wireless broadband with over 100Mbps mobile capacity and 1Gbps stationary bandwidth supported by OFDM, MIMO, and

software defined radio, Steer presents new 3G's components that will upgrade it up to 4G. The idea of upgrading 4G is shared by two other groups working on the next generation technology 3GPP and 3GPP2 developing new versions of UMTS and CDMA2000 cellular systems respectively. After introducing HSDPA (High-Speed Downlink Packet Access) in release 5, HSUPA (High-Speed Uplink Packet Access) in release 6, and HSOPA (High Speed OFDM Packet Access) in release 7, the 3GPP group project is working on release 8 – the UMTS (Universal Mobile Telecommunications System) Revision 8 LTE (Long Term Evolution) that will introduce 4G on UMTS foundations. The 3GPP plans presented in Technical Report (TR) 25.913 that are going to be concluded in September 2007 [6] expects cell coverage between 5 to 30 km, latency below 100ms, 100 Mbps/50Mbps downlink/uplink data rate within 20MHz spectrum allocation, high performance mobility up to 120km/h that between networks can be increased as much as up to 500km/h. The same report signifies the importance of IPbased networks with support of MIMO and OFDMA. The Pioneer and Inventor of 3G/WiFi Convergence Systems and Technologies, Top Global USA, Inc. created the first such 4G picture, the first mobile router that links 3G/4G Cellular and Wi-Fi networks. Providing seamless routing and secure connectivity, Top Global's router maintains connection in moving vehicles with 802.11n, HSDPA, and WiMAX wireless access points simultaneously .

4. Conclusion

4G is all about integrated, global network that is based on an open system approach. At the moment we have several technologies each capable of performing some of functions like broadband data access in mobile or nomadic environment, supporting voice traffic using voice over IP etc. But what we really need is a deployment of new technologies that allow merging, bridging and integrating all these repeated system into an information delivery system of the twenty first century. 4G stands for fourth Generation cellular network. Nowadays, network technology plays a significant role on science and business area. Everyday new technologies are emerging. Fourth Generation (4G) is the next generation of wireless networks that will replace third Generation (3G) networks sometimes in future.

5. References

[1] B.Xu, S. Hischke and B. Walke. "The Role of Ad hoc Networking in Future Wireless Communications". In Proc. ICCT. Beijing, 2003.

[2] Mobile IP-based Network Develpoments (IST-2000-28584 MIND). Project homepage: http://www.ist-mind.org

[3] F. Bader, C. Pinart, C. Christophi, E. Tsiakkouri, I. Ganchev, V. Friderikos, C. Bohoris, L. Correia, L. Ferreira. "User-Centric Analysis of Perceived QoS in 4G IP Mobile/Wireless Networks". PIMRC'2003, Pp. x.1-x.7, 7-10 September 2003. Beijing, China. ISBN 0-7803-7823-7.

[4] F. Stajano and R. J. Anderson. —The resurrecting duckling: Security issues for ad-hoc wireless networks. In 7th Security Protocols Workshop, vol. 1796 of LNCS, UK, 1999. Springer-Verlag, Germany

[5] Yuh-Min Tseng. —A heterogeneous-network aided public- key management scheme for mobile ad hoc networksl, Published on 10 February 2006 in Wiley InterScience,Int. J. Network Mgmt; 17: 3–15

[6] S. Capkun, L. Buttyan and J-P Hubaux. "Self-Organized Public-Key Management for Mobile Ad Hoc Networks ", IEEE Transactions on Mobile Computing, Vol. 2, No. 1, Jan-Mar 2003, pp. 52-64

[7] Hussian S., Hamid Z., and Khattak N., " Mobility Management Challenges and Issues in 4G Heterogeneous Networks."

Volume 2, No. 6, June 2011
Journal of Global Research in Computer Science
REVIEW ARTICLE
Available Online at www.jgrcs.info
ISSN-2229-371X

ASSESSMENT OF SECURITY IN MOBILE AD-HOC NETWORKS (MANET)

Deepak Chayal*, Dr. Vijay Singh Rathore**

Research Scholar*, Director**
NIMS University, Jaipur*
S.K.College, Jaipur**
deepak_chahal@yahoo.co.in

Abstract: With the proliferation of cheaper, smaller, and more powerful mobile devices, mobile ad hoc networks (MANETs) have become one of the fastest growing areas of research. This new type of self-organizing network combines wireless communication with a high degree node mobility. Unlike conventional wired networks they have no fixed infrastructure (base stations, centralized management points and,the like). Mobile ad hoc networks (MANETs) are one of the fastest growing areas of research. Conventional networks use dedicated nodes to carry out basic functions like packet forwarding, routing, and network management. In ad hoc networks these are carried out collaboratively by all available nodes. In this paper, we'll discuss about the MANET specific attacks, security challenges, goals and protocols alongwith the techniques used to secure MANETs.

INTRODUCTION

Attacks on an ad hoc network routing protocols generally fall into one of two categories: routing disruption attacks and resource consumption attacks. In a routing disruption attack, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. In a resource consumption attack, the attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth, or to consume node resources such as memory (storage) or computation power. From an application layer perspective, both attacks are instances of a Denial-of-Service (DoS) attack. An attacker may attempt to make a route through itself appear longer by adding virtual nodes to the route; we call this attack *gratuitous detour*, as a shorter route exists and would otherwise have been used. In ad hoc network routing protocols that attempt to keep track of perceived malicious nodes in a "blacklist" at each node, such as is done in watchdog and pathrater [1], an attacker may *blackmail* a good node, causing other good nodes to add that node to their blacklists, thus avoiding that node in routes.

MANET SPECIFIC ATTACKS

The unique characteristics of MANET routing algorithms result in new sets of wireless computing attacks. The majority of these attacks are directed at the algorithmic capabilities; the means of communicating routing information and the transporting of data. A partial listing of MANET specific attacks follows:

Altering Radio Route Tables –
Hack the radio and modifying routing tables and the propagation of these alterations [2].

Black Listing –
Trick a network/system into believing a good node is behaving maliciously .

Jamming –
Selectively jamming routing messages that define the network. Jamming a central node can break down a network. Timed jamming at intervals can cause the appearance of messages being lost, route loss.

Jellyfish –
Active insertion of jitter/delay into packet routing harms QoS and can deny timely packet delivery[3].

Replay –
A node in a network may rebroadcast the energy from a neighboring node, extending its range. Thus node B, hearing the replayed message of A by C, will believe that the shortest route is through A. Nodes A and B have no knowledge that packets are being replayed. This is a type of Man in the Middle attack, classified as an unauthenticated node having inserted itself into the network function [4].

Selfish Node –
Nodes that refuse to fully participate in routing.

Sink Hole –
Taking on more routing than needed, forcing data thought it self; becoming an overly critical network node [5].

SECURITY CHALLENGES

Some of the security challenges in MANET are:

Channel vulnerability:
Broadcast Wireless channels allow message Eavesdropping and Injection easily.

Bnode vulnerability:
Nodes do not reside in physically protected places, thus easily fall under attack.

Absence of infrastructure:
Certification/ Authentication Authorities are absent.

Dynamically Changing Network Topology
Puts security of routing protocols under threat.

Power and Computational Limitations

Prevent the use of complex Encryption Algorithms.

SECURITY GOALS OF MANETs

At the highest level, the security goals of MANETs are not that different from other networks. Most typically authentication, confidentiality, integrity, availability, and non-repudiation.

Authentication

is the verification of claims about the identity of a source of information. Authenticity is essentially assurance that participants in communication are genuine and not impersonators. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operations of the other nodes [6].

Confidentiality

means that only authorized people or systems can read or execute protected data or programs. It should be noted that the sensitivity of information in MANETs may decay much more rapidly than in other information.

Integrity

Means that the information is not modified or corrupted by unauthorized users or by the environment. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [7]: *Malicious altering and Accidental altering.*

Availability

Refers to the ability of the network to provide services as required. The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of the security state of it.

Non-Repudiation

ensures that committed actions cannot be denied. In MANETs security goals of a system can change in different modes (e.g. peace time, transition to war, and war time of a military network). The characteristics of MANETs make them susceptible to many new attacks. At the top level attacks can be classified according to network protocol stacks.

Access control/ authorization:

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users.

Anonymity:

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

Scalability:

Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

SECURE AD HOC ROUTING PROTOCOLS

Several researchers have proposed secure routing protocols. Several routing protocols have been proposed for routing in ad hoc networks; however, until recently, security in such networks has not yet enjoyed much attention from the research community. As a result, ad hoc network routing protocols that assume a trusted environment are highly vulnerable to attack; for example using the wormhole or rushing attacks, an adversary can paralyze ad hoc networks.

SEAD [8]

The Secure Efficient Ad hoc Distance Vector (SEAD) is a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector (DSDV) algorithms. To developing SEAD, follow the table driven approach. In table driven routing protocol maintain at all times routing information regarding to the network connectivity of every node to all other nodes. It is also known as proactive routing protocol.

SRP [9]

Secure Routing Protocol (SRP) was developed based on Destination Source Routing protocol (DSR). The operation of SRP requires the existence of a Security association (SA) between source node initiating a route query and the destination node. The security association can be utilized in order to establish a shared secret key between the two nodes, which is used by SRP.

ARIADNE

Ariadne is a secure routing protocol developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig based on the Dynamic Source Routing protocol (DSR). Ariadne is an on-demand routing protocol, which find routes as when it required, dynamically. Ariadne uses MAC s and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime. It contains two phases in its routing mechanism; Route discovery and Route maintenance. In the route discovery phase the source node establishes a route by flooding route request packets (RREQ).

ARAN

The Authenticate routing for ad hoc network (ARAN) is a secure routing protocol for MANETs, developed by Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz and Elizabeth M. Belding-Royer based on AODV. ARAN

utilizes cryptography mechanism in order to achieve security goals such as; authentication, message integrity, and non-repudiation in ad-hoc networks. It uses asymmetric cryptography to securing routing in an ad hoc network and require universal trusted third party.

SOADV [10]

Secure Ad hoc On-demand Distance Vector (SAODV) is a proposal for security extensions to the AODV protocol. The proposed extensions utilize digital signatures and hash chains in order to secure AODV packets. In order to facilitate the transmission of the information required for the security mechanisms, SAODV defines extensions to the standard AODV message format. SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts. Tunneling attacks are possible through two compromised nodes. Wormhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible reply attacks.

TECHNIQUES USED TO SECURE MOBILE AD-HOC NETWORKS

In order to provide solutions to the security issues involved in mobile ad-hoc networks, we must elaborate on the two of the most commonly used approaches in use today:

Prevention

Prevention dictates solutions that are designed such that malicious nodes are thwarted from actively initiating attacks. Prevention mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information. Among the existing preventive approaches, some proposals use symmetric algorithms, some use asymmetric algorithms, while the others use one-way hashing, each having different trade-offs and goals. Prevention mechanisms, by themselves cannot ensure complete cooperation among nodes in the network.

Detection and Reaction

Detection on the other hand specifics solutions that attempt to identify clues of any malicious activity in the network and take punitive actions against such nodes. All protocols in this category are designed such that they are able to detect malicious activates and react to the threat as needed.

CONCLUSION

The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers. A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range uses intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication to automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

REFERENCES

[1] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. In Proceedings of the Sixth Annual IEEE/ACM International Conference on Mobile Computing and Networking (MobiCom 2000), pages 255–265, August 2000.

[2] K. Sanzgiri, B. Dahill, B.N. Levine, E. Royer, and C. Shields. "A Secure Routing Protocol for Ad Hoc Networks" Technical Report 01-37, Department of Computer Science, University of Massachusetts, August 2001.

[3] I. Aad, J. Hubaux, and E. Knightly. "Denial of Service Resilience in Ad Hoc Networks," ACM MobiCom, September 2004.

[4] M. Brumster, and T. Le. "Optimistic Tracing in MANET," Florida State University, Department of Computer Science, March 2006.

[5] A. Burg. "Ad hoc Network Specific Attacks," Ad hoc networking: Concepts, Applications and Security Seminar, Technische Universität München, 2003.

[6] L. Gong. Increasing availability and security of an authentication service. IEEE Journal on Selected Areas in Communications, 11(5):657–662, June 1993.

[7] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.

[8] Y-C Hu, D. B. Jhonson, and A. Perrig, " SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Network," in Poceeding of 4th IEEE workshop on Mobile Computing System and Applications.

[9] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Network," in Proc. of CNDS 2002.

[10] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad hoc Wireless Network," Mobile Computing, T. Imielinski and H. Korth, Ed. Kluwer, 1996.

IJCTA-Menu

- Author Instructions
- Editorial Board
- Current Issue
- Call for paper
- Peer Review Process
- Indexing

Downloads

- Author Instructions
- Copyrights Form
- Paper

News and Updates

Dear Professors,Researchers, and scientist, research articles,review articles and short communications are invited for the July-August issue of International Journal of Computer Technology and Applications (IJCTA)

OPEN ACCESS

Search

IJCTA ©

Current language: English

Login:

Password:

Sign in. Register

IC Journals Master List
Journal of the Week
Journals Master List
Recently Added Journals
Top 100 Journals
Publishers
Top 20 Publishers
Journal Search
Evaluation methodology
FAQ
Contact

IC Conferences
Conferences

IC Journals Master List 2010
Advertisement
Advertisement purchase

Submission Menu
Register Journal
- Free Service
IC Publisher Panel

IndexCopernicus Search Journals

Back

Search results

Found: 36 records

NEXT 20

Title	ISSN	INDEX COPERNICUS 2010
Advances in Computational Research	0975-9085	4.47
Advances in Computer Science and Engineering	0973-6999	6.34
IETE Journal of Research	0377-2063	9.78
IETE Technical Review	0256-4602	9.56
IJAEST - INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES	2230-7818	4.79
Indian Journal of Library and Information Science	0973-9548	0.00
Information Science and Technology	0976-9188	4.00
International Journal of Advanced Computer and Mathematical Sciences	2230-9624	2.95
International Journal of Advanced Research in Computer Science	0976-5697	5.42
International Journal of Advancements in Technology	0976-4860	4.28
International Journal of Applied Engineering Research	0975-4259	4.07
International Journal of Applied Research on Information Technology and Computing	0975-8070	5.02
International Journal of BioSciences and Technology	0974-3987	3.85
International Journal of Computational Intelligence Techniques	0976-0474	4.47
International Journal of Computer Science and Information Technologies	0975-9646	4.21
International Journal of Computer Technology and Applications	2229-6093	4.67
International Journal of Engineering Science and Technology	0975-5462	3.14

International Journal of Computer Technology and Applications

ISSN: 2229-6093

2/18, Valmiki Street, Gandhi nagar, Saligramam, Chennai
Tamilnadu, INDIA
Email: - editor@ijcta.com
Website: - http://www.ijcta.com

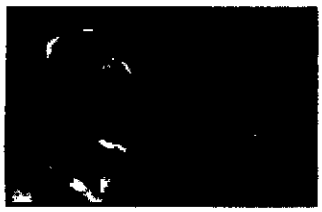
16/June/2011

Manuscript Acceptance letter

Dear Deepak Chalal,

Your Manuscript entitled **"Security Enhancement in MANET with 4G"** has been accepted for publication in the **July-August 2011 (Volume 2 Issue 4)** of IJCTA.Kindly pay the processing fee of Rs.3200. Kindly send the processing charge and duly signed copyrights form for further proceedings.

- CHIEF EDITOR



International Journal of Computer Technology and Applications

ISSN: 2229-6093

2/18, Valmiki Street, Gandhi nagar, Saligramam, Chennai
Tamilnadu, INDIA
Email: - editor@ijcta.com
Website: - http://www.ijcta.com

16/June/2011

Manuscript Acceptance letter

Dear Deepak Chalal,

Your Manuscript entitled **"Security Enhancement in MANET with 4G"** has been accepted for publication in the **July-August 2011 (Volume 2 Issue 4)** of IJCTA.Kindly pay the processing fee of Rs.3200. Kindly send the processing charge and duly signed copyrights form for further proceedings.

- CHIEF EDITOR

Security Enhancement in MANET with 4G

Mr. Deepak Chayal*, Dr. Vijay Singh Rathore**
Research Scholar, Professor***
*Department of Computer Science, NIMS University, Jaipur**
*Department of Computer Science, S.K. College, Jaipur***

ABSTRACT

Ad hoc networks seem to have commercial potential in business meeting places, hotspots, home environments and personal areas allowing fast exchange of documents during meetings, exchange of data when playing games in a group of users and connecting home appliance among other uses. In the context of the heterogeneous and integrated 4G environment, ad hoc networking is considered an important solution to extend the radio coverage of wireless systems and multimedia Internet services to wireless environments. 4G Technology is basically the extension in the 3G technology with more bandwidth and service offers in the 3G. The expectation for the 4G technology is basically the high quality audio/video streaming over end to end Internet Protocol. As the need for fastest communication is the foremost priority of present era also the need of quick data transfer, distant business correspondence by sharing data becomes very important. In this paper, we've dealt with the primary challenge of building security in MANETs and also maintain the information required to properly route traffic. Along with this, we have also discussed about the potentials of 4G technology.

1. Introduction to Available Wireless Technologies

Traditionally, the service provision in 2G networks, e.g. GSM, has been mainly based on voice services, closed business model support and limited operator differentiation due to a narrow set of offered services. Actually, mobile service provision is facing important advancements towards more flexible business models, with the introduction of new 2.5G/3G generations of mobile communication systems, like GPRS, UMTS and CDMA2000. Unfortunately, these 2.5/3G networks entail limitations to fulfill requirements imposed by current mobile users specially with the "anytime, anywhere with anybody" type of communication. Since 1970s, the research of ad hoc networking was mainly large scale networks for emergency/rescue and military purposes respectively for disaster and battlefield communication applications. *Large scale isolated ad hoc networks* are not suited to transport a large amount of data due to their very low traffic performance, slow topology convergence and security problems. However, these could be used to transport very urgent short messages (e.g. to inform about the location of an accident or to transmit tactical commands). Since 1990s, *small isolated ad hoc networking* has been experiencing a growing interest in the commercial and residential areas due the proliferation of small information computational devices and the emerging wireless technologies (IEEE 802.11, Bluetooth). This development is driven by the need to exchange digital information among people in direct contact enabled by ad hoc networking among a number or wireless nodes. Small In the context of the heterogeneous and integrated 4G environment, ad hoc networking is considered an important solution to extend the radio coverage of wireless systems and multimedia Internet services to wireless environments [1],[2]. In these *integrated ad hoc networks* mobile ad hoc hosts and routers can gain Third/fourth generation cellular networks (3G/4G) are broadband wireless mobile networks that has evolved from the 1st to the 2nd and 3rd generation networks. The still evolving 4th generation network is expected to be deployed in later 2011.

2. The Fourth Generation Technology

4G is short for Fourth (4th) Generation Technology. 4G Technology is basically the extension in the 3G technology with more bandwidth and service offers in the 3G. The expectation for the 4G technology is basically the high quality audio/video streaming over end to end Internet Protocol. If the Internet Protocol (IP) multimedia sub-system movement achieves what it going to do,

nothing of this possibly will matter. 4G is intended to provide:

- High speed
- High capacity
- Low cost per bit
- IP based services for video, data and voice (VoIP).

4G is all about integrated, global network that is based on an open system approach. At the moment we have several technologies each capable of performing some of functions like broadband data access in mobile or nomadic environment, supporting voice traffic using voice over IP etc[3]. But what we really need is a deployment of new technologies that allow merging, bridging and integrating all these repeated system into an information delivery system of the twenty first century. 4G stands for Fourth Generation and is the latest technology with high speed transferability of data with security measurements. It is coming with wireless broadband for the instant download. Talking about the standard of 4G technology, so far, two technologies are supposed to be the features of 4G.

2.1.WiMAX

WiMAX stands for Worldwide Interoperability of Microwave Access previously worked as fixed wireless facility under the 802.16e band. Now the modified standard 802.16m has been developed with the properties of speed, wide spectrum, and increase bandwidth. 4G has an advantage of having the WiMAX as a product because IEEE has introduced and released it already, therefore its economic as there is no need to pay for its manufacturing price. 4G supports two basic equipments;W iMAX Network system (network infrastructure) and mobile phone set. Smartphones with Wireless Access introduced in the market are the model 4G mobiles. These smartphones are equipped with the wireless internet accessibility and there is no fear of losing connection while travel from one tower to another tower range. WiMAX or mobile structural design will become progressively more translucent, and therefore the acceptance of several architectures by a particular network operator ever more common.

2.2. LTE

Parallel to WiMAX, LTE (Long Term Evolution) is introduced by Verizon. LTE is considered to be promising high data transfer speed. LTE is supposed to provide internet facility using both systems. It has the ability of transition from one mode to another. LTE is developed on radio waves technology. This not only increases the speed but also the amount of data allowed through the same bandwidth and results into lower cost. As LTE is compatible with 3G technology so, it not only increases the speed but also prevents the need of new network and can work through the same infrastructure. LTE will not only support the functions of 3G but also incorporate some newer ones. LTE is using MIMO (Multiple input multiple output) and is able to send and receive huge data. It is negative in the sense that it will overload the base stations networks.

4G Technology offers high data rates that will generate new trends for the market and prospects for established as well as for new telecommunication businesses. 4G networks, when tied together with mobile phones with in-built higher resolution digital cameras and also High Definition capabilities will facilitate video blogs. After successful implementation, 4G technology is likely to enable ubiquitous computing, that will simultaneously connect to numerous high data speed networks offering faultless handoffs all over the geographical regions. Many network operators possibly utilize technologies for example; wireless mesh networks and cognitive radio network to guarantee secure connection & competently allocates equally network traffic and bandwidth.

3. Security Enhancement in MANET with 4G

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Authentication research has determined that for a positive identification, elements from at least two, and preferably all three, factors be verified. The three factors (classes) and some of elements of each factor are:

3.1.The Ownership Factors:

Something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone).

3.2. The Knowledge Factors:

Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question))

3.3. The Inherence Factors:

Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

At small scale, the identity verification can be managed by the nodes themselves, as handshaking by virtue of their proximity [4], but at relatively larger scale it becomes complex and the nodes identity verification demands the authentication involvement of TTP [5]. There are schemes that are based on the concept of self-organization in MANETS [6] thoroughly without TTP connection where the identity is resolved by the nodes themselves or some hybrid form of above two schemes might be used [4].

The 4G system was originally envisioned by the Defense Advanced Research Projects Agency. The DARPA selected the distributed architecture, end-to-end Internet protocol (IP), and believed at an early stage in peer-to-peer networking in which every mobile device would be both a transceiver and a router for other devices in the network eliminating the spoke-and-hub weakness of 2G and 3G cellular systems. Since the 2.5G GPRS system, cellular systems have provided dual infrastructures: packet switched nodes for data services, and circuit switched nodes for voice calls. In 3g and 4G systems, the circuitswitched infrastructure is abandoned, and only a packetswitched network is provided. This means that traditional voice calls are replaced by IP telephony. Cellular systems such as 4G allow seamless mobility; thus a file transfer is not interrupted in case a terminal moves from one cell (one base station coverage area to another, but handover is carried out. The terminal also keeps the same IP address while moving, meaning that a mobile server is reachable as long as it is within the coverage area of any server. In 4G systems this mobility is provided by the mobile IP protocol, part of IP version 6, and while in earlier cellular generations it was only provided by physical layer and data link layer protocols. In addition to seamless mobility, 4G provides flexible interoperability of the various kinds of existing wireless networks, such as satellite, cellular wireless, WLAN, PAN and systems for accessing fixed wireless networks. 4G stands for the fourth-generation cellular network. Although it is generally agreed that 4G is going to offer better communication technology than 3G, it is still undefined as to which areas should be really improved upon, and in which ways, from 3G. Researchers are often pointing towards integration whereas business institutions are working on upcoming technologies that will make 4G more attractive to the business community by implementing it more customer-friendly. New support for mobility is the primary concern of Hussian *et. al.* [7] and they pointed out insufficient 3G mobility constrained by bandwidth that should be significantly increased. According to them, the significant progress that 4G can achieve in the area of mobility is unifying different and currently separated environments into a single fixed OWA (Open Wireless Architecture) that will achieve high connectivity by accessing all kinds of networks. Providing single terminal that will effectively access the best available internet connection will increase and speed up device usability under 4G. Integration is the key concept in defining 4G capabilities since we should support all kinds of multimedia by offering single access to all wireless networks. Understanding the significance of unifying Wi- Fi, WiMax and Cellular networks into one product, Woerner and Howlader proposed that the most important factor of 4G will be "seamless integration of wireless networks" based on flexibility of the software radio technology, with improved bandwidth capacity, and improved routing techniques allowing multi-hop peer-topeer networks. Due to the lack of single military scenario where and how 4G will be used, it is critical that future wireless technology will be capable of effortlessly accessing all kind of radio communications. Bauer *et. al.* addressed that enhanced cellular range and capacity, supported by Wi-Fi and WiMAX networks is the vision of 4G. However, considering the fast development of WiMAX networks, and the increasing range of Wi-Fi standards, they argue that these new wireless networks can in the future substitute cellular networks such as the current 3G. They also addressed that it is "misleading" calling the evolution of cellular technology in terms of generations because this would "suggest a linear progression" which is not the case. Finally, they also evaluated business opportunities of 4G pointing out on establishing a global standard, along with open architecture, and supporting multiple interfaces all over the world, as the keys to economical success. Steer [7] addressed 4G is officially designated by IEEE as "Beyond 3G." Characterized by wireless broadband with over 100Mbps mobile capacity and 1Gbps stationary bandwidth supported by OFDM, MIMO, and software defined radio, Steer presents new 3G's components that will upgrade it up to 4G. The idea of

upgrading 4G is shared by two other groups working on the next generation technology 3GPP and 3GPP2 developing new versions of UMTS and CDMA2000 cellular systems respectively. After introducing HSDPA (High-Speed Downlink Packet Access) in release 5, HSUPA (High-Speed Uplink Packet Access) in release 6, and HSOPA (High Speed OFDM Packet Access) in release 7, the 3GPP group project is working on release 8 – the UMTS (Universal Mobile Telecommunications System) Revision 8 LTE (Long Term Evolution) that will introduce 4G on UMTS foundations. The 3GPP plans presented in Technical Report (TR) 25.913 that are going to be concluded in September 2007 [6] expects cell coverage between 5 to 30 km, latency below 100ms, 100 Mbps/50Mbps downlink/uplink data rate within 20MHz spectrum allocation, high performance mobility up to 120km/h that between networks can be increased as much as up to 500km/h. The same report signifies the importance of IPbased networks with support of MIMO and OFDMA. The Pioneer and Inventor of 3G/WiFi Convergence Systems and Technologies, Top Global USA, Inc. created the first such 4G picture, the first mobile router that links 3G/4G Cellular and Wi-Fi networks. Providing seamless routing and secure connectivity, Top Global's router maintains connection in moving vehicles with 802.11n, HSDPA, and WiMAX wireless access points simultaneously .

4. Conclusion

4G is all about integrated, global network that is based on an open system approach. At the moment we have several technologies each capable of performing some of functions like broadband data access in mobile or nomadic environment, supporting voice traffic using voice over IP etc. But what we really need is a deployment of new technologies that allow merging, bridging and integrating all these repeated system into an information delivery system of the twenty first century. 4G stands for fourth Generation cellular network. Nowadays, network technology plays a significant role on science and business area. Everyday new technologies are emerging. Fourth Generation (4G) is the next generation of wireless networks that will replace third Generation (3G) networks sometimes in future.

5. References

[1] B.Xu. S. Hischke and B. Walke. "The Role of Ad hoc Networking in Future Wireless Communications". In Proc. ICCT. Beijing. 2003.

[2] Mobile IP-based Network Develpoments (IST-2000-28584 MIND). Project homepage: http://www.ist-mind.org

[3] F. Bader, C. Pinart, C. Christophi, E. Tsiakkouri, I. Ganchev, V. Friderikos, C. Bohoris, L. Correia, L. Ferreira. "User-Centric Analysis of Perceived QoS in 4G IP Mobile/Wireless Networks". PIMRC'2003, Pp. x.1-x.7, 7-10 September 2003. Beijing, China. ISBN 0-7803-7823-7.

[4] F. Stajano and R. J. Anderson. —The resurrecting duckling: Security issues for ad-hoc wireless networks. In 7th Security Protocols Workshop, vol. 1796 of LNCS. UK, 1999. Springer-Verlag. Germany

[5] Yuh-Min Tseng. —A heterogeneous-network aided public- key management scheme for mobile ad hoc networksl, Published on 10 February 2006 in Wiley InterScience,Int. J. Network Mgmt; 17: 3–15

[6] S. Capkun, L. Buttyan and J-P Hubaux. "Self-Organized Public-Key Management for Mobile Ad Hoc Networks ", IEEE Transactions on Mobile Computing, Vol. 2, No. 1, Jan-Mar 2003, pp. 52-64

[7] Hussian S., Hamid Z., and Khattak N., " Mobility Management Challenges and Issues in 4G Heterogeneous Networks."